

## UNITED STATES DISTRICT COURT

for the

District of Oregon

Portland Division

In the Matter of the Search of )  
 (Briefly describe the property to be searched )  
 or identify the person by name and address )  
 The premises located at 13225 SW Falcon Rise Drive, )  
 Tigard, Oregon 97223, more fully described in )  
 Attachment A hereto )

Case No.

18-MC-47

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon  
 (identify the person or describe the property to be searched and give its location):

The premises located at 13225 SW Falcon Rise Drive, Tigard, Oregon 97223, more fully described in Attachment A hereto

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

**YOU ARE COMMANDED** to execute this warrant on or before Feb 6, 2018 (not to exceed 14 days)  
 in the daytime 6:00 a.m. to 10:00 p.m.  at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stacie F. Beckerman, via the Clerk's Office  
 (United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person whose property, will be searched or seized (check the appropriate box)

for \_\_\_\_\_ days (not to exceed 30)  until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued: Jan. 23, 2018 2:32 pm

City and state: Portland, Oregon

  
 Judge's signature

Honorable Stacie F. Beckerman, U.S. Magistrate Judge

Printed name and title

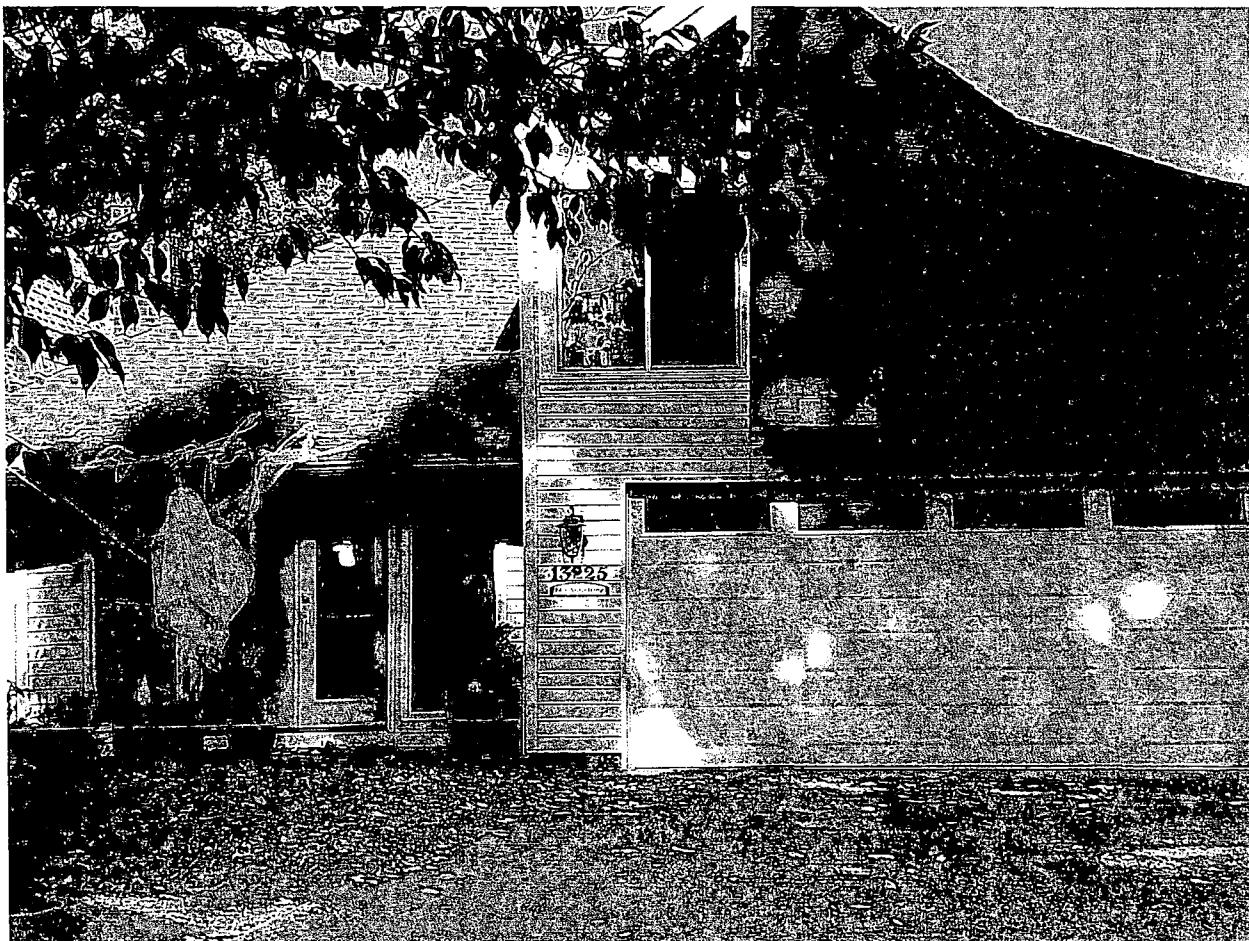


**ATTACHMENT A**

**Description of Location to be Searched**

**The Premises Located at 13225 SW Falcon Rise Drive, Tigard, Oregon 97223, including Outbuildings, Garages, and Storage Sheds Associated with those Premises**

13225 SW Falcon Rise Drive, Tigard, Oregon 97223, is a two story wood framed single family residence with an attached two car garage. The residence is light green in color with white trim and a brown composition roof. The front door of the residence faces SW Falcon Rise Drive and is comprised primarily of a glass panel surrounded by light colored wood. The black numbers "13225" are affixed to the left of the garage door. Directly below the numbers is a black and white "No soliciting" sign.



**ATTACHMENT B**

**Items to be Searched For, Seized, and Examined**

The following records, documents, and items that constitute contraband and evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), namely the transportation, distribution and possession of child pornography.

1. **Records, Documents, and Visual Depictions:**

- a. Any and all records, documents, or materials, including correspondence, that pertain to the transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
- b. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
- c. Any and all motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;
- d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

e. Any and all records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs.

h. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received, and the like.

2. **Digital Evidence:**

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes referenced above, or to create, access, or store contraband or evidence, fruits, or instrumentalities of such crimes, including central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards,

printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices such as modems, routers, cables, and connections; storage media; and security devices;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes referenced above, or to create, access, process, or store contraband or evidence, fruits, or instrumentalities of such crimes;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, thumb drives, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store contraband, or evidence, fruits, or instrumentalities of such crimes;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

As used herein, the terms "records," "documents," "programs," "applications," or "materials" include records, documents, programs, applications, or materials created, modified, or stored in any form.

### **Search Procedure**

In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a. *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and herein.

b. *On-site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and herein. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any

data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data

device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.